D4

(12) UK Patent Application (19) GB (11) 2 375 872 (13) A

(43) Date of A Publication 27.11.2002

(21) Application No 0112480.9

(22) Date of Filing 22.05.2001

(71) Applicant(s)
Vodafone Group Services Limited
(Incorporated in the United Kingdom)
The Courtyard, 2-4 London Road,
NEWBURY, Berks, RG14 1JX,
United Kingdom

(72) Inventor(s)
Nicholas Bone

(74) Agent and/or Address for Service
Mathisen Macara & Co
The Coach House, 6-8 Swakeleys Road,
Ickenham, UXBRIDGE, Middlesex,
UB10 8BZ, United Kingdom

(51) INT CL^7
G07F 7/08

(52) UK CL (Edition T)
G4V VAK
G4T TBX

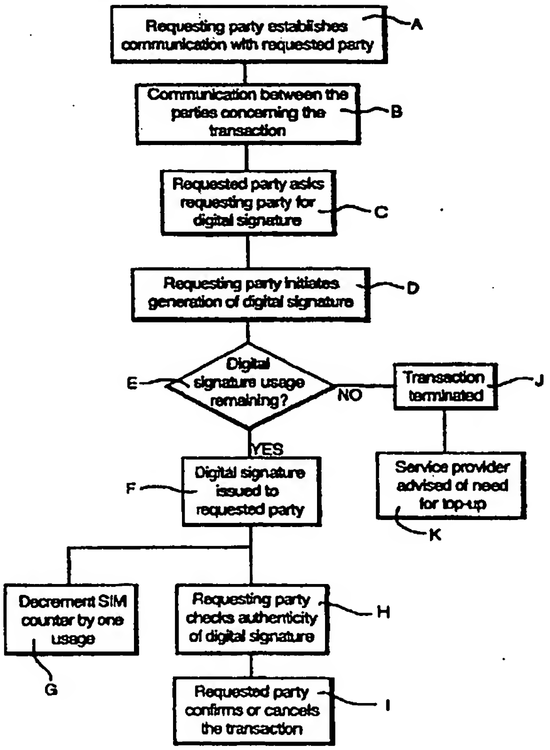
(56) Documents Cited
None

(58) Field of Search
UK CL (Edition S) G4T TBX, G4V VAK
INT CL^7 G07F 7/08 7/10
ONLINE: EPODOC, JAPIO, WPI

(54) Abstract Title
Electronic transaction systems and methods

(57) Electronic transaction systems and methods are described in which a mobile telephone user ("requesting party") uses their handset to enter into an electronic transaction with another party ("requested party"), which may be a commercial transaction for the supply of goods or services to the requested party in return for payment or may involve no payment (e.g. requesting entry into a building). The system and method may be employed in a mobile telecommunication or telephone system such as a GSM or UMTS (3G) system. The requesting party's mobile terminal or handset is provided with a digital signature by a service provider (which may be the network operator), and the requesting party issues this digital signature to the requested party for identification purposes as part of the transaction. Each issuance of the digital signature is recorded in a counter in the handset which may be incorporated into its SIM or smart card or equivalent. The counter may be periodically set by the service provider to allow a predetermined number of digital signature usages which can be pre-paid (such as in the case of a pre-pay mobile telephone subscriber) or which can be billed to the subscriber (in the case of a contract, non-pre-pay, subscriber). When the allowed number of digital signature usages has taken place, this may be signalled to the subscriber and/or to the service provider so that action can then be taken to top-up the counter again, for payment.

Fig.1.


Requesting party establishes communication with requested party
A
Communication between the parties concerning the transaction
B
Requested party asks requesting party for digital signature
C
Requesting party initiates generation of digital signature
D
E
Digital signature usage remaining?
NO
Transaction terminated
J
YES
F
Digital signature issued to requested party
Service provider advised of need for top-up
K
Decrement SIM counter by one usage
Requesting party checks authenticity of digital signature
H
G
Requested party confirms or cancels the transaction
I

GB 2 375 872 A

At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.

Fig.1.

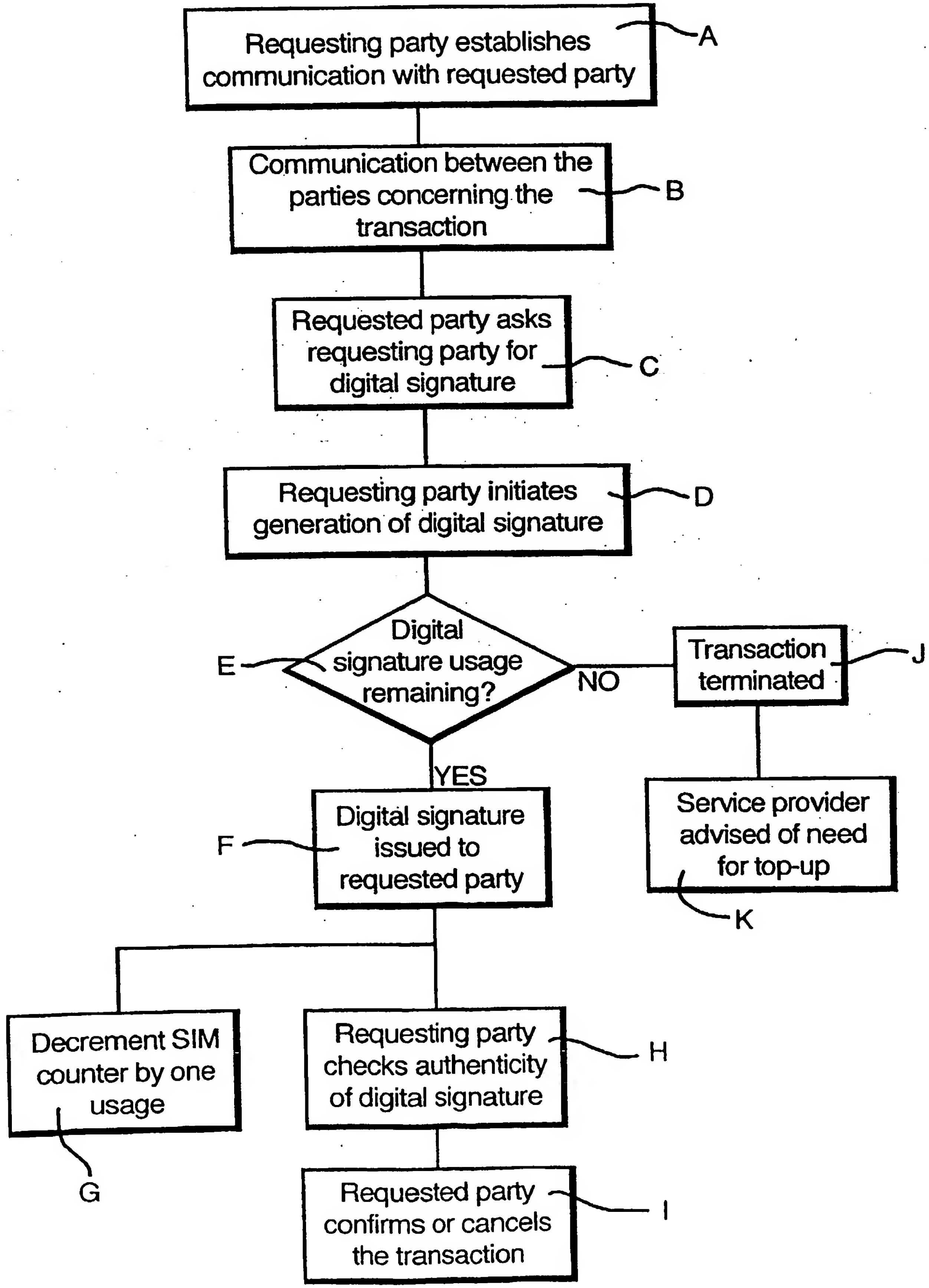

Requesting party establishes communication with requested party
A
Communication between the parties concerning the transaction
B
Requested party asks requesting party for digital signature
C
Requesting party initiates generation of digital signature
D
Digital signature usage remaining?
E
NO
Transaction terminated
J
YES
Digital signature issued to requested party
F
Service provider advised of need for top-up
K
Decrement SIM counter by one usage
G
Requesting party checks authenticity of digital signature
H
Requested party confirms or cancels the transaction
I

Fig.2.

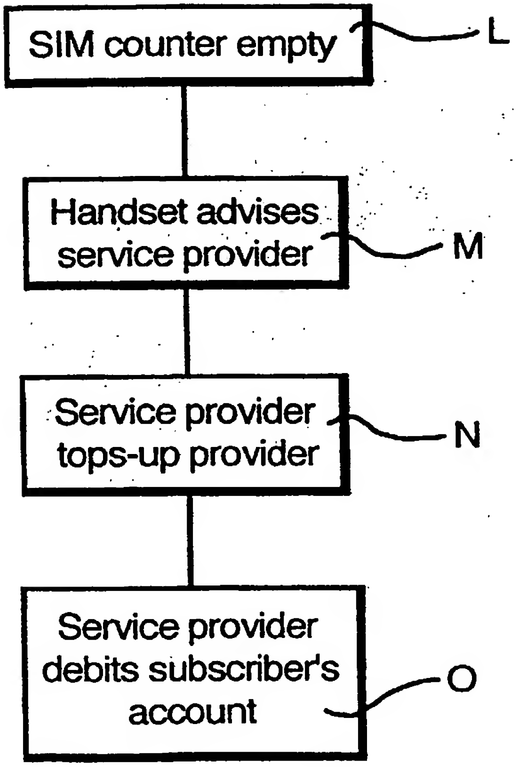
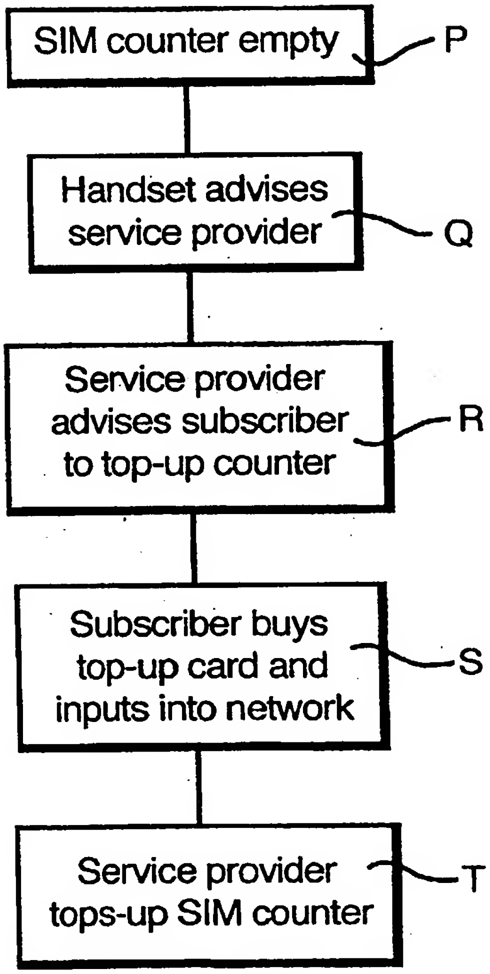

SIM counter empty
L
Handset advises service provider
M
Service provider tops-up provider
N
Service provider debits subscriber's account
O

Fig.3.


SIM counter empty
P
Handset advises service provider
Q
Service provider advises subscriber to top-up counter
R
Subscriber buys top-up card and inputs into network
S
Service provider tops-up SIM counter
T

ELECTRONIC TRANSACTION SYSTEMS AND METHODS

The invention relates to electronic transaction systems and methods. Systems and methods according to the invention, to be described in more detail below by way of example only, relate to electronic transactions which involve the use of a digital signature for authorisation purposes. The term "transaction" involves an interaction between two (or more) parties but is not necessarily an interaction involving payment by one party to another party.

According to the invention, there is provided an electronic transaction method for use in electronic transactions each of which involves a requesting party and a requested party, in which the requesting party issues to the requested party an identifying signal previously provided by a third party, each issuance of the identifying signal by a particular requesting party being registered in a manner which becomes known to the third party.

According to the invention, there is also provided an electronic transaction system for use in electronic transactions each of which involves a requesting party and a requested party, comprising issuing means controlled by the requesting party for issuing to the requested party an identifying signal previously provided by a third party, and registering means for registering each issuance of the identifying signal by a particular requesting party in a manner which becomes known to the third party.

According to the invention, there is further provided a smart card for use in a mobile terminal of a telecommunications or telephone system, arranged to record a count value representing a number of issuances by that terminal of a digital signature identifying that terminal or its user.

Systems and methods according to the invention for use in carrying out electronic transactions will now be described, by way of example only, with reference to the accompanying drawings in which Figures 1,2 and 3 thereof show flow charts of operations carried out in the systems and methods.

Electronic transactions may take various different forms. Normally, there will be two parties involved (other parties may be indirectly involved as will be explained). In such a transaction, for example, one party ("the requested party") is in possession or control of the intended subject-matter of the transaction and a second party ("the requesting party") wishes to obtain that subject-matter. The subject-matter may be a physical object (e.g. a product which the second party wishes to purchase) or abstract (such as a service or information which the second party wishes to purchase). However, transactions may not necessarily involve a payment. For example, payment may already have been made; or no payment at all may be involved - for example, the subject-matter of the transaction might relate to controlled entry into a building or area. In all these types of transactions, though, it is necessary for the requesting party to be identified to the satisfaction of the requested party. Where the transaction involves a payment from the requesting party to the requested party, the requested party requires the identity of the requesting party to be confirmed to a sufficient extent as to authorise the payment in a manner satisfactory to the requested party. If the transaction does not necessarily involve any payment by the requesting party to the requested party, the requested party nevertheless needs to have sufficient confirmation of the identity of the requesting party before being able to agree to release the subject-matter of the transaction to the requesting party. For example, if the requesting party is requesting entry into a building, the requested party will not be willing to allow this without being sufficiently certain of the identity of the requesting party.

It is known in such electronic transactions to use digital signatures for the purpose of establishing the required identity. Such a digital signature may be generated by the second party using "Public Key Infrastructure" (PKI), in which the requesting party uses their private key to produce the digital signature. The requested party obtains the requesting party's public key in the form of a Certificate issued by a Certificate Authority, and can then decrypt the digital signature, and can confirm the identity of the requesting party using the information in the Certificate.

Such an arrangement envisages, therefore, that the requesting party is provided with a digital signature for the purposes of entering into transactions of this type, and that this digital signature is authorised such as by a Certificate Authority as explained above. The service of providing digital signatures to requesting parties (or potential requesting parties) may be carried out by a service provider, who will wish to levy a charge for this service. One such arrangement of this type will now be more specifically described, and relates to the case where the service provider is providing telecommunication or telephone services to subscribers. The term "service provider" includes the network operator or an intermediary between the network operator and the subscribers. In a more specific example, the telecommunications or telephone network is a mobile network, and each subscriber is provided with a mobile terminal, such as a telephone handset. When such a subscriber wishes to enter into a transaction of the general type described above, as the requesting party, the subscriber will set up communication with the requested party using the handset. In order to confirm the transaction, the requesting party will then need to sign the transaction using a digital signature which will have been provided for this purpose by the service provider. For example, the digital signature would have been stored by the service provider in the handset and, more specifically, would have been stored on the SIM (Subscriber Identity Module) or smart card used in the handset if the network is of the GSM type. The requesting party can initiate the sending of the digital signature to the requested party by entering a personal identity number (PIN) into the handset, or by some other secure initiating means such as a biometric signature particular to the requesting party. Upon receipt of the digital signature, the requested party can then check its authenticity in the manner described, by reference to a Certificate issued by a Certificate Authority, and decide whether to confirm the transaction.

As described so far, the transaction proceeds without reference to the service provider. Nevertheless, the service provider has set up the digital signature for the subscriber and will normally wish to be reimbursed in respect thereof.

In the system being described, therefore, it is arranged that a charge is made for each use of the digital signature (or can, in principle, be made for each such use). In accordance with a feature of the invention as applied to a GSM telephone or telecommunications system, each use of the digital signature by a subscriber is recorded on the subscriber's SIM and, by means of an exchange of information between the SIM and the service provider, a charge can be made in the manner to be described. More specifically, the SIM may be provided with a counter (implemented by software) which can be credited with a number representing a predetermined number of available usages of the digital signature. The subscriber can pay in advance or in arrears in respect of number of uses of the digital signature stored in the counter. Thus, for example, the subscriber could pay in advance in the same manner as for pre-pay telephone usage, purchasing a specific number of digital signature usages (such as by means of a "top-up card" or by means of a credit card or other suitable means), and then communicating information relating to this purchase to the service provider in respect of his particular telephone handset (identified by the telephone number). The service provider then resets the counter on the subscriber's SIM using over-the-air signals.

For contract subscribers (that is, non-prepay subscribers), the counter could be topped up in the same way by the service provider, except that the charge would appear on the subscriber's next invoice instead of being paid in advance.

The re-setting of the counter (topping-up) to provide more credits could be initiated automatically (e.g. when all the available digital signature usages have been used, or when a predetermined low number of them remains) and/or could take place at the request of the subscriber. In the case of contract (non pre-pay subscribers, the topping-up process could be invisible to the subscriber.

As described above, transactions which require the use of the requesting party's digital signature can be transactions for the supply of goods or services which require the requesting party to pay for those goods or services, or they can be transactions (e.g. entry into a building) where no payment from the requesting party to the requested party is required. In principle, however, the service provider can charge for each usage of the digital signature by the requesting party, whether the transaction itself involves any payment or not.

However, it is also possible for the charge for usage of the digital signature to be levied not against the subscriber (requesting party) but against someone else, in particular, against the requested party. For example, in the case of a transaction involving the purchase of goods or services, the merchant (requested party) may agree to pay or reimburse the requesting party for use of the digital signature. In such a case, the requested party will advise the service provider who will then provide a "free" credit on the counter in the subscriber's SIM. Instead, for example, where a particular requested party agrees to pay for all digital signature usages by all or by specified subscribers, the service provider can maintain a count of all such digital signature usages by the respective subscribers and credit their SIMs accordingly. Of course, such an arrangement is also possible where the transaction does not involve any payment by the requesting party to the requested party. For example, if a subscriber (requesting party) is using the digital signature to obtain access into a building (for no payment), the owner of the building may agree to pay the service provider for each such digital signature usage in the manner explained.

Figure 1 shows an example of a transaction using digital signature in the manner explained above.

At step A, the requesting party uses his mobile handset to establish communication with the requesting party. At step B, communication takes place between the parties in relation to the transaction, for example, relating to the price, quantity, and availability of the subject-matter of the transaction.

At step C, the requested party asks for the requesting party to provide their identity to allow the transaction to be authorised. At step D, the requesting party initiates the generation of their digital signature (for example, by entering a PIN). At step E, the handset checks the status of the digital signature usage counter in the SIM. If at least one usage remains, the requesting party's handset issues the digital signature to the requested party (step F). At the same time, at step G, the digital signature usage counter in the SIM is decremented by one usage. At step H, the requested party checks the authenticity of the digital signature, such as by means of a Certificate issued by a Certificate Authority as explained above. Depending on the results of this authenticity check, at step I the requested party either confirms or cancels the transaction.

If step E determines that no digital signature usage remains available, at step J the requesting party terminates the transaction. At step K, the requesting party's handset may cause a signal to be sent to the service provider to initiate topping-up of the usage counter in the SIM.

The procedure described above envisages that the counter in the SIM, recording the number of available digital signature usages, is not being topped up automatically. If it is being topped up automatically, then steps E,J and K will be omitted - because there will always be available digital signature usages.

Figure 2 shows steps involved in topping up the digital signature usage counter in the SIM for a contract (non pre-pay) subscriber. At step L, the number of available digital signature usages remaining reaches zero, or some predetermined low number. At step M, the handset transmits a corresponding signal to the service provider. At step N, the service provider transmits a signal back to the SIM to top up the counter accordingly. At step O, an appropriate charge is debited to the subscriber by the system's billing procedure.

Figure 3 shows the corresponding procedure for topping-up the digital signature usage counter in the subscriber's SIM where the subscriber is a pre-pay subscriber.

At step P, the number of digital signature usages remaining reaches zero or some predetermined low number. At step Q, the handset transmits a corresponding signal to the service provider. At step R, the service provider sends a message to the subscriber, via the handset (e.g. by SMS), advising that the digital signature usage counter must be topped-up. At step S, the subscriber purchases further digital signature usage and inputs this into the network (via a top-up card or credit card or other suitable means). At step T, the service provider tops up the SIM counter.

Step Q could be omitted, and the counter on the SIM could itself directly generate the message advising the subscriber that the counter on the SIM must be topped up.

In the transactions described, the digital signature need not of course identify the subscriber as an individual but may instead merely identify the subscriber's handset.

The telephone system to which the invention may be applied is not necessarily a GSM system. It may, for example, be an UMTS (3G) system. In such a case, the digital signature usage counter would be embodied in the smart cards used in such systems. However, it will be understood that various modifications may be made to the system and methods described without departing from the scope of the invention. The invention is not restricted to mobile telephone or telecommunications systems, and is not restricted to telephone handsets using SIMs. It may be used in other circumstances where a service provider providing a digital signature (or other secure identification) can set up communication between and with the user of the digital signature or other secure identification.

CLAIMS

1. An electronic transaction method for use in electronic transactions each of which involves a requesting party and a requested party, in which the requesting party issues to the requested party an identifying signal previously provided by a third party, each issuance of the identifying signal by a particular requesting party being registered in a manner which becomes known to the third party.

2. A method according to claim 1, in which the issuances of the identifying signal by a particular requesting party are counted, and the count value is assessed by the third party from time to time.

3. A method according to claim 2, in which the third party applies a releasable block against further issuance of the identifying signal by a particular requesting party when the count value reaches a predetermined level.

4. A method according to claim 3, in which the third party releases the block for payment.

5. A method according to claim 4, in which the payment is made or to be made by the requesting party.

6. A method according to claim 4, in which the payment is made or to be made by the requested party.

7. A method according to claim 4, in which the payment is made or to be made by a fourth party.

8. A method according to any one of claims 2 to 7, in which the identifying signal issued by a particular requesting party is issued by equipment controlled by that party, and in which the said count is made and stored at or by that equipment and transmitted to the third party from time to time for the assessment.

9. A method according to claim 8, in which the equipment is part of a telecommunications or telephone system.

10. A method according to claim 9, in which the telecommunications or telephone system is a mobile system.

11. A method according to claim 8, in which the equipment is a mobile terminal or handset employing a smart card, and in which the count is stored on the smart card.

12. A method according to any preceding claim, in which the identifying signal is a digital signature.

13. An electronic transaction system for use in electronic transactions each of which involves a requesting party and a requested party, comprising issuing means controlled by the requesting party for issuing to the requested party an identifying signal previously provided by a third party, and registering means for registering each issuance of the identifying signal by a particular requesting party in a manner which becomes known to the third party.

14. A system according to claim 13, comprising counting means for counting the issuances of the identifying signal by a particular requesting party, and control means for enabling assessment of the count value by the third party from time to time.

15. A system according to claim 15, comprising blocking means for applying a releasable block against further issuance of the identifying signal by a particular requesting party when the count value reaches a predetermined level.

16. A system according to claim 15, comprising releasing means controlled by the third party for releasing the block for payment.

17. A system according to claim 16, in which the payment is made or to be made by the requesting party.

18. A system according to claim 16, in which the payment is made or to be made by

the requested party.

19. A system according to claim 16, in which the payment is made or to be made by a fourth party.

20. A system according to any one of claims 14 to 19, in which the issuing means is equipment controlled by the requesting party, and in which the counting means is part of that equipment.

21. A system according to claim 20, in which the equipment is part of a telecommunications or telephone system.

22. A system according to claim 21, in which the telecommunications or telephone system is a mobile system.

23. A system according to claim 20, in which the equipment is a mobile terminal or handset employing a smart card, and in which the counting means is embodied on the smart card.

24. A system according to any one of claims 13 to 23, in which the identifying signal is a digital signature.

25. A smart card for use in a mobile terminal of a telecommunications or telephone system, arranged to record a count value representing a number of issuances by that terminal of a digital signature identifying that terminal or its user.

26. A smart card according to claim 25, arranged to cause the mobile terminal to transmit the acummulated count value or a signal representative thereof to a service provider.

27. A smart card according to claim 24 or 25, arranged to apply a releasable block to further issuance by the mobile terminal of the digital signature until permitted by a signal received from the service provider.

28. A smart card according to claim 27, including storing means storing a limit value representing a maximum predetermined number of issuances of the digital signature by the terminal, the smart card being arranged to apply the releasable block when the count value reaches the limit value.

29. A mobile terminal in a telecommunications or telephone system, including a smart card according to any one of claims 25 to 28.

30. A mobile terminal according to claim 29, in a GSM or UMTS telephone system.

31. An electronic transaction method, substantially as described with reference to the accompanying drawings.

32. An electronic transaction system, substantially as described with reference to the accompanying drawings.

33. A smart card for use in a mobile terminal of a telecommunications or telephone system, substantially as described with reference to the accompanying drawings.

PATENTS • DESIGNS • The Patent Office • COPYRIGHT • TRADE MARKS

INVESTOR IN PEOPLE

17

Application No:	GB 0112480.9	**Examiner:**	Trevor Berry
Claims searched:	1 to 33	**Date of search:**	5 December 2001

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.S): G4T (TBX); G4V (VAK)

Int Cl (Ed.7): G07F 7/08, 7/10

Other: ONLINE: EPODOC, JAPIO, WPI

Documents considered to be relevant:

Category	Identity of document and relevant passage	Relevant to claims
	NONE	

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
		E	Patent document published on or after, but with priority date earlier than, the filing date of this application.
&	Member of the same patent family		